IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

KADEMI, LLC, a Mississippi limited liability company, SUPERIOR SERVICES INVESTMENT GROUP, LLC, a Georgia limited liability company, FOREST EXPRESS PROPERTIES, LLC, a Georgia limited liability company, JUST REV, LLC, a Georgia limited liability company, PIERCE N TELL OF SARASOTA, LLC, a Florida limited liability company, MARTIN'S AUTO REPAIR, a Georgia partnership, MOJO MAMA'S LLC, a Missouri limited liability company, YOUNG'S DISTRIBUTING CO., INC., a Missouri corporation, COASTAL COMMUNICATIONS, LLC, a Texas limited liability company, THE MELLO GROUP, INC., a Delaware corporation, DAWN LEA CHALMERS, RICHARD ALEXANDER, AKBAR ALI, POONAM ALI, REEVNEY ST. LUC, OSHIK PEREZ, TERESA SUE MARTIN, WILLIAM MARVIN MARTIN, JR., ANGELA M. KROUT, BRIDGETTE YOUNG, JEFF NEWKIRK, CHRIS WILLIAMS, individually and on behalf of others similarly situated, Plaintiffs,	Case No.:____________ Complaint--Class Action JURY TRIAL DEMANDED

v.	)
	)
EQUIFAX, INC.,	)
	)
Defendant.	)
	)

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiffs Kademi, LLC, Superior Services Investment Group, LLC, Forest Express Properties, LLC, Just Rev, LLC, Pierce N Tell of Sarasota, LLC, Martin's Auto Repair, Mojo Mama's LLC, Young's Distributing Co. Inc., Coastal Communications, LLC, The Mello Group, Inc. (the "Small Business Plaintiffs"), Dawn Lea Chalmers, Richard Alexander, Akbar Ali, Poonam Ali, Reevney St. Luc, Oshik Perez, Teresa Sue Martin, William Marvin Martin, Angela M. Krout, Bridgette Young, Jeff Newkirk, and Chris Williams (the "Consumer Plaintiffs), (hereinafter, collectively, "Plaintiffs"), individually and on behalf of the Classes defined below, allege the following against Equifax, Inc. ("Equifax") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

SUMMARY OF CASE

1. This case is being brought on behalf of small businesses across the United States and their owners against Equifax for damages (current and future) resulting

from the September 2017 cybersecurity incident ("Data Breach") that impacted approximately 143 million individuals and their businesses.

2. At all times material, Equifax knew that identity theft has been a major problem in the United States and victims lose billions of dollars each year. Identity theft and financial fraud is not limited to consumers. Businesses are also targeted in identity theft and other fraudulent financial schemes, i.e. known as Business or Corporate Identity Theft. The State of Colorado, for example, has warned:

> Identity theft is a crime that affects over 9 million people and costs over $56 billion to the economy every year, according to the Better Business Bureau. Identity theft impacts many consumers around the country and in Colorado. However, consumers are no longer the only targets of identity thieves.
>
> Business identity theft (also known as corporate or commercial identity theft) is a new development in the criminal enterprise of identity theft. In the case of a business, a criminal will hijack a business's identity and use that identity to establish lines of credit with banks or retailers. With these lines of credit, the identity thieves will purchase commercial electronics, home improvement materials, gift cards, and other items that can be bought and exchanged for cash or sold with relative ease.
>
> The damage can be devastating to the victim's business. The damage to the victim's credit history can lead to denial of credit, which can lead to operational problems. The cost to clean up and correct the damage can be hundreds of dollars and hours of lost time.[1]

One of the tips that the State of Colorado provides to business owners to avoid becoming a victim of business identity theft is:

> Never provide an employer identification number (EIN), social security number, financial information, or personal information to anyone

[1] https://www.sos.state.co.us/pubs/business/ProtectYourBusiness/BITresourceguide.html

> unless you have initiated the contact and have confirmed the requesting business or the person's identity. (Emphasis added)[2]

3. To try and prevent business identity theft, Experian, a credit bureau like Equifax, states on its website:

> Business identity theft and fraud losses cost American companies billions each year. Both can negatively impact cash flow, cause problems with creditors and suppliers and even affect your business's reputation.
>
> The first step in business identity theft protection is to regularly check your company's credit report for unusual activity that might indicate identity fraud. Enroll in a monitoring service of your company's credit report so you can regularly inspect it for atypical activity that might be a sign of fraud. Experian has an identity theft protection service called Business Credit Advantage[SM] which offers unlimited access to your credit report for a one year. It monitors your profile every day and emails you warnings of any changes to your business credit report or score.[3]

4. Unlike consumers who are entitled under federal law to obtain one free credit report annually, however, business must pay for their credit reports. For example, Experian charges between $39.95 per business credit report and/or $149 annually for the Business Credit Advantage plan referenced above. Equifax charges $99 per business credit report.

5. As has been well publicized in the news recently, Equifax was hacked by criminals and as a result, personally identifiable information ("PII"), including

---

[2] Id.

[3] http://www.experian.com/small-business/business-credit-scores.jsp

names, Social Security numbers, birth dates, addresses. driver's license numbers and credit card numbers was stolen.

6. Many of the 143 million individuals whose PII was hacked are also owners of small businesses that heavily rely on personal and business credit to operate and provide for families across this country. Any business with fewer than 500 employees is generally defined as a small business – a definition adopted by the U.S. Census Bureau, the Bureau of Labor Statistics, the Federal Reserve and the Small Business Administration.[4] There are about 28 million small businesses in America representing more than 99% of all American companies.[5] Indeed, small businesses employ half of the private sector work force, and since 1995, small businesses have created about two out of every three net new jobs – 65% of the total job creation in the United States.[6]

7. Business loans and credit have historically been critical for small businesses to survive because, unlike large firms, small businesses lack access to public institutional debt and equity capital markets. According to the Harvard Business School Article referenced in footnote 4, in 2012, over 85% of small businesses

---

[4] Mills, Karen and McCarthy, Brayden, *The State of Small Business Lending: Credit Access During the Recovery and How Technology May Change the Game* (Harvard Business School, 2014) (the "Harvard Business School Article").

[5] *Id*. citing U.S. Census Bureau, SUSB and nonemployer statistics.

[6] *Id*.

reported to the National Federation of Independent Businesses (the "NFIB") that their primary financial institution was either a large or community bank.[7]

8. In addition, according to the NFIB, about 60% of small businesses use loans to finance their operations, and use the loan capital for a variety of purposes, ranging from maintaining cash flow and working capital to purchasing equipment and financing real estate purchases.[8]

9. The ability of small businesses to obtain loans and other forms of credit is dependent on the creditworthiness of the business owner.[9] As a result, small businesses were hit the hardest during the 2008 financial crisis, and were the slowest to recover. One reason for this is that business owners' personal financial condition deteriorated during the financial crisis causing a decrease in the amount of collateral that could be pledged by the business owner to the lender for the business loan. In addition, ever since the financial crisis, increased regulatory oversight has dampened the ability of small businesses to obtain credit because of stricter underwriting criteria, which includes heightened scrutiny of the business owners'

[7] *Id.* at 17.

[8] *Id.* citing to *National Federation of Independent Businesses, "Small Business, Credit Access and a Lingering Recession* (January 2012).

[9] For example, the United States Small Business Administration requires all businesses applying for an SBA loan to submit a personal financial statement for the business owner as part of the loan application process. In other words, the creditworthiness of a small business is dependent upon the creditworthiness of its owner.

creditworthiness.[10] Therefore, as it relates to the continued viability of small businesses being able to obtain business credit, for small businesses to grow and for our nation's economy to flourish, it was/is imperative that Equifax honor its responsibility to protect the PII of consumers and business owners so that individuals and businesses can continue to exist without the threat of being a victim of identity theft, fraudulent loans and other financial frauds.

10. As a credit bureau that is responsible for determining the creditworthiness of individuals and businesses, it was certainly foreseeable to Equifax prior to the most recent Data Breach that the dissemination of the PII of business owners has placed the creditworthiness of the businesses at substantial risk of business identity theft and, as set forth in more detail below, has caused damages to the impacted businesses, including but not limited to theft of personal and financial information, unauthorized charges, out-of-pocket expenses incurred to monitor their personal and business credit, etc.

11. Based on the allegations above and below, the Consumer Plaintiff and Small Business Plaintiffs and their respective Class Members are seeking to certify two nationwide classes, a Consumer Class and Small Business Class, to hold Equifax responsible for the damage caused to them and this country by the most recent Data Breach.

---

[10] *Id*. at 4.

NATURE OF CASE

12. Plaintiffs bring this class action case against Defendant Equifax for its failure to safeguard consumers' and small business owners' personally identifiable information ("PII"), which has damaged both the Consumer Plaintiffs and Small Business Plaintiffs.

13. Equifax is a credit bureau that collects, stores, analyzes and sells products and services based on consumer and business credit information. In its most recent Form 10-K that was filed on February 22, 2017, Equifax states:

> Equifax is a leading global provider of information solutions and human resources business process outsourcing services for businesses. Governments and consumers…. Our products and services are based on comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data.[11]

14. As it relates to the Small Business Plaintiffs, the comprehensive database of information that Equifax collects and stores on businesses includes and is based in part on the PII that was recently hacked in the Data Breach. Equifax has acknowledged that a cybersecurity incident ("Data Breach") potentially impacted approximately 143 million individuals.

---

[11] Form 10-K filed by Equifax, Inc. on February 22, 2017 (emphasis added).

15. It has also acknowledged that unauthorized persons exploited a website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 consumers, and certain dispute documents with personal identifying information for approximately 182,000 consumers, were accessed. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but has failed to inform the public why it delayed notification of the Data Breach to the public.

16. To date, Equifax has not acknowledged that the Data Breach has also damaged the businesses that are owned by many of these same consumers. Indeed, the Small Business Plaintiffs have been harmed by the Data Breach separate and apart from the Consumer Plaintiffs, because businesses have their own separate credit scores and reports. In the case of small businesses, generally defined by the U.S. Small Business Administration as businesses with 500 employees or fewer, the creditworthiness of each small business and the Small Business Plaintiffs is dependent on the creditworthiness of its owner(s) whose PII Equifax has admitted was hacked by criminals.

17. Equifax could have prevented this Data Breach and has exposed Plaintiffs to, at a minimum, substantial risk of harm.

18. The Data Breach was the result of Equifax's inadequate approach to data security and the protection of the Consumer Plaintiffs' and Small Business Plaintiffs' PII that it collected during the course of its business.

19. Equifax disregarded the rights of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

20. As a result of the Equifax Data Breach, the PII of both the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members has been exposed to criminals for misuse.

21. The injuries suffered or likely to be suffered by the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members are separate and distinct and were caused as a direct result of the Equifax Data Breach. The injuries include but are not limited to:

a. unauthorized use of the PII of the Consumer Plaintiffs and Small Business Plaintiffs;

b. theft of the Consumer Plaintiffs' and Small Business Plaintiffs' personal and financial information;

c. costs associated with the detection and prevention of the Consumer Plaintiffs and Small Business Plaintiffs identity theft and unauthorized use of the Consumer Plaintiffs and Small Business Plaintiffs financial accounts;

d. damages arising from the inability of the Consumer Plaintiffs and Small Business Plaintiffs to use their PII;

e. loss of use of and access to the Consumer Plaintiffs' and Small Business Plaintiffs' account funds, as well as costs associated with inability of the Consumer Plaintiffs and Small Business Plaintiffs to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. the costs incurred by the Consumer Plaintiffs and Small Business Plaintiffs, which are associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

g. the imminent and certainly impending injury flowing from the substantial risk of potential fraud and identify theft posed to the Consumer Plaintiffs and Small Business Plaintiffs by their PII being placed in the hands of criminals and already misused via the sale of the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' information on the Internet black market;

h. damages to and diminution in value of the Consumer Plaintiffs and Small Business Plaintiffs PII collected and sold by Equifax; and

i. the loss of the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' privacy.

22. The injuries to the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII.

23. Further, the Consumer Plaintiffs and Small Business Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Equifax is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII was stolen as a result of the Equifax Data Breach.

24. The Consumer Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. The Consumer Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

25. The Small Business Plaintiffs bring this action based on common law negligence and negligence per se to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. The Small Business Plaintiffs seek the following remedies, among others: reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class

members. And, at least some members of the proposed Class have a different citizenship from Equifax.

27. This Court has personal jurisdiction over Equifax because Equifax maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Georgia.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax 's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' claims occurred in this District.

PARTIES

29. Plaintiff Kademi, LLC, is a limited liability company existing under the laws of the state of Mississippi. Plaintiff Kademi, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Kademi, LLC is dependent on the creditworthiness of Plaintiff Dawn Lea Chalmers. Plaintiff Kademi, LLC is a small retail company. Plaintiff Kademi, LLC has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

30. Plaintiff Superior Services Investment Group, LLC is a limited liability company existing under the laws of the state of Georgia. Plaintiff Superior Services Investment Group, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Superior Services Investment Group, LLC is dependent on the creditworthiness of Plaintiff Richard Alexander. Plaintiff Superior Services Investment Group, LLC is a real estate business services company based in Georgia. Plaintiff Superior Services Investment Group, LLC has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

31. Plaintiff Forest Express Properties, LLC is a limited liability company existing under the laws of the state of Georgia. Plaintiff Forest Express Properties, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Forest Express Properties, LLC is dependent on the creditworthiness of Plaintiffs Akbar Ali and Poonam Ali. Plaintiff Forest Express Properties, LLC is a small business that purchases and sells real estate. Plaintiff Forest Express Properties, LLC has suffered damages, at a minimum, by having to spend time and effort monitoring its financial accounts.

32. Plaintiff Just Rev, LLC is a limited liability company existing under the laws of the state of Georgia. Plaintiff Just Rev, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Just Rev, LLC

is dependent on the creditworthiness of Plaintiff Reevney St. Luc. Plaintiff Just Rev, LLC is a small music business. Plaintiff Just Rev, LLC has suffered damages, at a minimum, by having to spend time and effort monitoring its financial accounts.

33. Plaintiff Pierce N Tell of Sarasota, LLC is a limited liability company existing under the laws of the state of Florida. Plaintiff Pierce N Tell of Sarasota, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Pierce N Tell of Sarasota, LLC is dependent on the creditworthiness of Plaintiff Oshik Perez. Plaintiff Pierce N Tell of Sarasota, LLC is a small retail company. Plaintiff Pierce N Tell of Sarasota, LLC has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

34. Plaintiff Martin's Auto Repair is a partnership existing under the laws of the state of Georgia. Plaintiff Martin's Auto Repair is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Martin's Auto Repair is dependent on the creditworthiness of Plaintiffs Teresa Sue Martin and William Marvin Martin, Jr. Plaintiff Martin's Auto Repair is a small business that repairs automobiles. Plaintiff Martin's Auto Repair has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

35. Plaintiff Mojo Mama's, LLC is a limited liability company existing under the laws of the state of Missouri. Plaintiff Mojo Mama's, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Mojo Mama's, LLC is dependent on the creditworthiness of Plaintiff Angela M. Krout. Plaintiff Mojo Mama's, LLC is a small retail company. Plaintiff Mojo Mama's, LLC has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

36. Plaintiff Young's Distribution Co., Inc., is a limited liability company existing under the laws of the state of Missouri. Plaintiff Young's Distribution Co., Inc. is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Young's Distribution Co., Inc. is dependent on the creditworthiness of Plaintiff Bridgette Young. Plaintiff Young's Distribution Co., Inc. is a small retail company. Plaintiff Young's Distribution Co., Inc. has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

37. Plaintiff Coastal Communications, LLC, is a limited liability company existing under the laws of the state of Texas. Plaintiff Coastal Communications, LLC is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff Coastal Communications, LLC is dependent on the creditworthiness of Plaintiff Jeff Newkirk. Plaintiff Coastal Communications, LLC

is a small communications company. Plaintiff Coastal Communications, LLC has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

38. Plaintiff The Mello Group, Inc., is a limited liability company existing under the laws of the state of Delaware. Plaintiff The Mello Group, Inc. is a victim of the Data Breach and relies, in part, on credit to operate. The creditworthiness of Plaintiff The Mello Group, Inc. is dependent on the creditworthiness of Plaintiff Chris Williams. Plaintiff The Mello Group, Inc. is a small business management consulting company. Plaintiff The Mello Group, Inc. has suffered damages, at a minimum, by having to purchase a business credit report and spend time and effort monitoring its financial accounts.

39. Plaintiff Dawn Lea Chalmers is a resident of the state of Mississippi. She is a victim of the Data Breach. Plaintiff Dawn Lea Chalmers is the owner of Kademi, LLC. Plaintiff Dawn Lea Chalmers has spent time and effort monitoring her financial accounts.

40. Plaintiff Richard Alexander is a resident of the state of Georgia. He is a victim of the Data Breach. Plaintiff Richard Alexander is the owner of Superior Services Investment Group, LLC. Plaintiff Richard Alexander has spent time and effort monitoring his financial accounts.

41. Plaintiffs Akbar Ali and Poonam Ali are residents of the state of Georgia. They are victims of the Data Breach. Plaintiffs Akbar Ali and Poonam Ali are the owners of Forest Express Properties, LLC. Plaintiffs Akbar Ali and Poonam Ali have spent time and effort monitoring their financial accounts.

42. Plaintiff Reevney St. Luc is a resident of the state of Georgia. He is a victim of the Data Breach. Plaintiff Reevney St. Luc is the owner of Just Rev, LLC. Plaintiff Reevney St. Luc has spent time and effort monitoring his financial accounts.

43. Plaintiff Oshik Perez is a resident of the state of Florida. He is a victim of the Data Breach. Plaintiff Oshik Perez is the owner of Pierce N Tell of Sarasota, LLC. Plaintiff Oshik Perez has spent time and effort monitoring his financial accounts.

44. Plaintiffs Teresa Sue Martin and William Marvin Martin are residents of the state of Georgia. They are victims of the Data Breach. Plaintiffs Teresa Sue Martin and William Marvin Martin are the owners of Plaintiff Martin's Auto Repair. Plaintiffs Teresa Sue Martin and William Marvin Martin have spent time and effort monitoring their financial accounts.

45. Plaintiff Angela M. Krout is a resident of the state of Missouri. She is a victim of the Data Breach. Plaintiff Angela M. Krout is the owner of Mojo Mama's,

LLC. Plaintiff Angela M. Krout has spent time and effort monitoring her financial accounts.

46. Plaintiff Bridgette Young is a resident of the state of Missouri. She is a victim of the Data Breach. Plaintiff Bridgette Young is the owner of Young's Distributing Co., Inc. Plaintiff Bridgette Young has spent time and effort monitoring her financial accounts.

47. Plaintiff Jeff Newkirk is a resident of the state of Texas. He is a victim of the Data Breach. Plaintiff Jeff Newkirk is the owner of Coastal Communications, LLC. Plaintiff Jeff Newkirk has spent time and effort monitoring his financial accounts.

48. Plaintiff Chris Williams is a resident of the state of Florida. He is a victim of the Data Breach. Plaintiff Chris Williams is the owner of The Mello Group, Inc. Plaintiff Chris Williams has spent time and effort monitoring his financial accounts.

49. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above.

STATEMENT OF FACTS

A. Equifax is a heavily regulated credit bureau that is entrusted with non-public information on individuals and businesses and is required by law to protect the information that it collects from being the subject of data breaches.

50. Equifax, a global corporation, "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."[12]

51. Equifax is one of three nationwide credit-reporting companies that track and rates the creditworthiness of individuals and businesses. As a credit bureau service, Equifax maintains information related to the credit history of consumers and businesses and for example, provides the information to creditors who are considering a borrower's application for credit or who have extended credit to the borrower.

52. Equifax gets its data from multiple sources including but not limited to credit card companies, banks, retailers, and lenders who report on the credit activity of individuals and businesses, as well as by purchasing public records.

53. As described by Equifax:

> [B]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debt management and human resources-related services. We also offer products that enable individual consumers to manage their financial affairs and protect their identity.[13]

[12] (http://www.equifax.com/about-equifax/company-profile/ (September 11, 2017)).

[13] Equifax's 2016 Annual Report at 12.

54. Among other federal and state laws applicable to Equifax that are designed to protect Plaintiffs from having their PII stolen, Equifax is a "financial institution" pursuant to the Gramm-Leach-Bliley Act ("GLBA"), and as such GLBA imposes "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801; *see also TransUnion LLC v. F.T.C*, 295 F.3d 42, 48 (D.C. Cir. 2002). To satisfy this obligation, Equifax was at all times material required and failed to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. 15 U.S.C. § 6801 (b)

55. At all times material, Equifax was required and failed to comply with 16 C.F.R. §314.4 by failing to adequately:

- Develop, implement, and maintain a comprehensive information security program that is: (1) written in one or more readily accessible parts, and (2) contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue;

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement information safeguards to control the risks [they] identify through risk assessment, and regularly oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate, safeguards for the customer information at issue; and test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (2) Requiring [their] service providers by contract to implement and maintain such safeguards.
- Evaluate and adjust [their] information security program in light of the results of the testing and monitoring required by circumstances that [they] know or have reason to know may have a material impact on [their] information security program.

B. Equifax also sells products to third parties that are based on the creditworthiness of individuals and businesses.

56. In addition to being a credit bureau, Equifax derives substantial revenue by selling products that are based on the creditworthiness of individuals and businesses. For example, in its 2016 Annual Report, Equifax states, in part:

> Businesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debt management and human resources-related services. We also offer a portfolio of products that enable individual consumers to manage their financial affairs and protect their identity. Our revenue stream is diversified among businesses across a wide range of industries, international geographies and individual consumers.
>
> The U.S. Information Solutions (USIS) segment, the largest of our four segments, consists of three service lines: Online Information Solutions; Mortgage Solutions; and Financial Marketing Services. Online Information Solutions and Mortgage Solutions revenue is principally transaction-based and is derived from our sales of products such as consumer and commercial credit reporting and scoring, identity management, fraud detection and modeling services. USIS also markets certain decisioning software services, which facilitate and automate a variety of consumer and commercial credit-oriented decisions. Financial Marketing Services revenue is principally project and subscription based and is derived from our sales of batch credit and consumer wealth information such as those that assist clients in acquiring new customers, cross selling to existing customers and managing portfolio risk.[14]

57. Equifax charges different prices for these products. For example, with regard to obtaining an individual credit report, Equifax's website states that "[f]ederal law requires each of the three nationwide credit reporting agencies (CRAs) - Equifax,

[14] 2016 Equifax Annual Report, pg. 12.

Experian and TransUnion – to give you a free credit report every 12 months if you ask for it."[15] Thereafter, Equifax charges between $17.95 and $29.95 per month for credit reports, credit monitoring and financial alerts, i.e. Equifax Complete Premier Plan, Equifax Complaint Family Plan and Equifax Complete Advantage Plan.[16]

58. With regard to credit reports on businesses, Equifax does not provide business owners or consumers with a free report. Equifax charges $99 for a credit report on a business. All the other credit bureaus such as FICO and Experian also charge for business credit reports.

59. To date, despite admitting that the PII of approximately 143 million individuals (including business owners) was stolen, Equifax has offered nothing to business owners who were impacted by the Data breach. For example, Equifax has not offered business owners products such as credit monitoring, credit freeze or even a free copy of their business's credit report to find out if their businesses have been harmed as a result of the breach. To date, business owners are required to pay Equifax $99 for a copy of their business credit report.

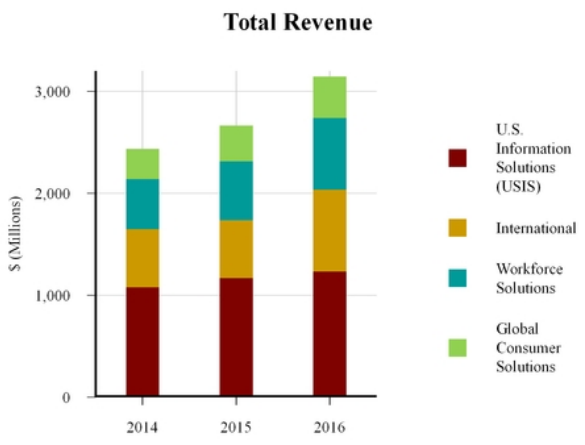
---

[15] https://www.equifax.com/personal/education/credit/score/how-to-check-credit-score

[16] *Id.*

60. Equifax financially benefits to the tune of over a billion dollars annually from the sale of its credit-related products for individuals and businesses. Equifax's 2017 Form 10-K states[17]:

> Our revenue base and business mix are diversified among our four segments as depicted in the chart below.


Total Revenue
3,000
2,000
1,000
0
$ (Millions)
2014
2015
2016
U.S. Information Solutions (USIS)
International
Workforce Solutions
Global Consumer Solutions

61. As a result, it was foreseeable to Equifax that the Data Breach would harm individual consumers and their businesses.

D. The Equifax Data Breach could be the worst in U.S. History.

62. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files."

[17] 2017 Equifax Form 10-K at pg. 3 filed on or about February 22, 2017; https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm

63. Included among those files was a treasure trove of personal data: names, dates of birth, Social Security numbers and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

64. Personal data like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

65. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII and non-public business information – a form of intangible property that Equifax collected and stored and that was compromised in and as a result of the Equifax Data Breach.

66. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

67. Moreover, the Consumer Plaintiffs and Small Business Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

68. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is

highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

69. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

70. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

71. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[18]

[18]Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

72. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

73. Equifax was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals and businesses who would be harmed by a breach of Equifax's systems.

74. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

75. The ramifications of Equifax's failure to keep Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' data secure are severe.

76. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[20]

---

[19] 17 C.F.R. §248.01 (2013).
[20] *Id.*

77. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

78. Identity thieves can use personal information, such as that of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

79. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[22]

80. Reimbursing a consumer or business for a financial loss due to fraud does not make that individual or business whole again. On the contrary, identity theft

---

[21] Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

[22] See https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraudhits-inflection-point (last visited April 10, 2017).

victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[23]

81. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

82. The Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[23] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).

[24] 7 GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

83. The PII of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

84. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Consumer Plaintiffs' and Small Business Plaintiffs' and Class their respective members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

85. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

86. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the

field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

87. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

88. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' PII, causing them to

suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of the Consumer Plaintiffs' and Small Business Plaintiffs' and their respective Class members' information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

89. Equifax has not offered any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages

sustained by the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members.

90. While the PII of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members has been stolen, Equifax continues to hold PII of consumers, including the PII of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members. Particularly because Equifax and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CHOICE OF LAW

91. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. residents against a company doing business in Georgia, has a greater interest in the claims of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

92. The principal place of business of Equifax, located at 1550 Peachtree Street NE Atlanta, Georgia 30309, is the centralized location of its business activities – the place where its high-level officers direct, control, and coordinate the corporation's

activities, including its data security, and where: a) major policy, b) advertising, c) distribution, d) accounts receivable departments and e) financial and legal decisions originate.

93. Furthermore, Equifax's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Georgia.

94. Equifax's breach of its duty to customers, the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members, emanated from Georgia. Application of Georgia law to a nationwide Class with respect to the claims of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

95. Further, under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia will apply to the common law claims of the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members.

CLASS ALLEGATIONS

96. The Consumer Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P.

23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seeks certification of a Nationwide class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Nationwide Class").

97. The Small Business Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), the Small Business Plaintiffs seeks certification of a Nationwide class defined as follows:

> All United States businesses whose creditworthiness is dependent on the creditworthiness of its business owners whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Nationwide Small Business Class").

98. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, the Consumer Plaintiffs and Small Business Plaintiffs assert claims under the laws of the individual States, and on behalf of separate statewide classes, defined as follows:

Statewide Consumer Class

> All persons residing in [STATE] whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Statewide Consumer Classes").

Statewide Small Business Class

> All United States businesses residing in [STATE] whose creditworthiness is dependent on the creditworthiness of its business owners whose personally

identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Statewide Small Business Class").

99. Excluded from each of the above Classes are Equifax and any of its Affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

100. The Consumer Plaintiffs and Small Business Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

101. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

102. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class include at least 143 million individuals whose PII was compromised in the Equifax Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

103. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Equifax had a duty to protect PII;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class members;

g. Whether the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and,

h. Whether the Consumer Plaintiffs and Small Business Plaintiffs and their respective Class members are entitled to relief.

104. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seeks relief consistent with the relief of the Class.

105. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

106. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be

encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

107. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

108. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify the public of the Breach;

b. Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the PII of Plaintiffs and the Class members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

109. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding he Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I

NEGLIGENCE (ON BEHALF OF ALL PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

110. Plaintiffs restate and reallege Paragraphs 1 through 109 as if fully set forth herein.

111. Upon accepting and storing the PII of Plaintiffs and Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

112. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

113. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

114. Equifax also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

115. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

116. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

117. Equifax breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class Members.

118. Because Equifax knew that a breach of its systems would damage

millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

119. Equifax had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

120. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

121. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the data breach.

122. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs' and Class members' PII had been improperly acquired or accessed.

123. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII and of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax possession or control.

124. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

125. Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of sthares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

126. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax's possession or control.

127. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

128. Upon information and belief, Equifax improperly and inadequately

safeguarded PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax'sfailure to take proper security measures to protect sensitive PII of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

129. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

130. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

131. As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach

and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

NEGLIGENCE PER SE (ON BEHALF OF ALL PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

132. Plaintiffs restate and reallege Paragraphs 1 through 109 as if fully set forth herein.

133. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to

protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

134. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

135. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

136. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

137. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

138. As a direct and proximate result of Equifax's negligence per se,

Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA") (ON BEHALF OF CONSUMER PLAINTIFFS ONLY AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

139. Plaintiffs restate and reallege Paragraphs 1 through 109 as if fully set forth here.

140. As individuals, Plaintiffs and Class member are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

141. Under the FCRA, a "consumer reporting agency" is defined as "any

person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

142. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

143. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

144. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data

was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

145. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

146. Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

147. The Federal Trade Commission ("FTC") has pursued enforcement

actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

148. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

149. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. See, e.g., 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their

duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

150. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

151. Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

152. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT IV

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT (ON BEHALF OF CONSUMER PLAINTIFFS ONLY AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

153. Plaintiffs restate and reallege Paragraphs 1 through 109 as if fully set

forth herein.

154. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

155. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

156. Plaintiffs and the Nationwide Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

157. Plaintiffs and the Nationwide Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT V

DECLARATORY JUDGMENT (ON BEHALF OF ALL PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

158. Plaintiffs restate and reallege Paragraphs 1 through 109 as if fully set forth herein.

159. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

160. Equifax still possesses PII pertaining to Plaintiffs and Class members.

161. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

162. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

163. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

164. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against EQUIFAX as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

c. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

This 4th day of October 2017.

/s/ Jason R. Doss
Jason R. Doss
Georgia bar No. 227117
Samuel T. Brannan
Georgia Bar No. 076688
The Doss Firm, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
(770) 578-1314 (Telephone)
(770) 578-1302 (Facsimile)
jasondoss@dossfirm.com

ATTORNEYS FOR PLAINTIFFS